Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

**Remarks as delivered by
The Honorable Stephanie O'Sullivan
Principal Deputy Director of National Intelligence**

Innovation and Diversity in the Cyber Fight

**Cyber Education Summit
Georgia Regents University, Augusta, Ga.
Thursday, October 15, 2015**

I have an affinity for the MacGyvers of the world: the folks who innovate and make do with what they've got on the ground; the people who are told no, who aren't taken seriously because their ideas are so fantastic, so out of this world that they are beyond what most can reason.

So, if I told you that you could have unlimited funds, as much time as you need and the team of your choosing, what could you do with that?

That question was answered fifty nine years ago today, when a team of ten unveiled to the world just what they could do under those circumstances. On 15 October, 1956, an eclectic team of computer programmers from IBM shared their high-level programming language with the coding community, and it changed the world.

The team had found a way to capture human intent, the way that we conceptualize a problem, and recast it in a way that is understandable, executable by the machine. They had invented Fortran. And it was the first step toward making computer programming accessible, understandable outside of the programming elite.

The language that they invented was the Rosetta Stone of computer programming. Coding, prior to Fortran was indecipherable for most and arduous for even the best programmers. Fortran unlocked a world of possibility by dramatically simplifying the coding process. The team did in three years what most people thought simply unattainable.

It is a poetic coincidence, therefore, that we are gathered here today on the very day that the gift of language was given to the burgeoning cyber community, because in front of me is another community that is flourishing, because we can stand on the shoulders of that Fortran team. And instead of simply marveling at how far you've come, how far we've come, you are

Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

pushing us even further.

You're creating the foundation upon which so many others will stand. So thank you. Thank you for taking up the mantle, for innovating, and for being bold, because unlike that incredible team of ten, we do not have unlimited time or resources. The threats we face are complex and growing, and budgets are not infinite. In fact, they are diminishing. But the variable that we can yet affect is the team we bring to that fight.

I said that the Fortran team was composed of ten programmers, but that is not entirely true. They certainly earned that title over the years they worked together, but in fact, in addition to a few coders there was a crystallographer, a cryptographer, a chess wiz, an employee lent from an aircraft manufacturer, a researcher borrowed from M.I.T., and a recent college graduate. The only requirement to make that team was problem solving skills and a drive to invent the unimaginable. So, the Fortran team's 'recipe for success' was diversity, fearlessness, and a little genius. And that is precisely what we need again today.

Although I am here as a representative of the Intelligence Community, this need exists across Federal government, and even across this nation. We are beset by some of the most diverse threats I have seen in my, more than, thirty years in the Intelligence Community. And as a community, as a nation, we are facing pervasive global instability as a result of those most diverse threats.

Each year, in open Congressional hearing, Director Clapper presents the Intelligence Community's assessment of worldwide threats, and for the past three years, cyber has been at the top of that list. And although we can fixate on discussions about a large, Armageddon-scale strike that cripples our infrastructure, our reality today is an ongoing series of low-to-moderate level cyber intrusions which will absolutely continue and will likely expand.

Threats to our national security and economic security are increasing in frequency, scale, sophistication, and severity of impact and is made all the more complex because cybercriminals, hacktivist collectives like Anonymous, and terrorist groups experimenting with hacking are operating on the same Internet as aggressors like North Korea and Iran, and Russia and China who are more sophisticated and could do real damage if they so choose.

Events of this past year are instructive; starting with the intrusions against Sands Casino and Sony Pictures, and continuing with the OPM breaches. It's clear that the threat is real. And yet, we don't do all we could to prevent those attacks. There are four concrete and simple steps we can take today to improve our cyber posture and two far more complex steps that Ithink are absolutely necessary to affect real change.

Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

So, here are the easy ones first. One: patch IT software obsessively. Most cyber intrusions are through well-known vulnerabilities in commonly-used software, which can be fixed with patches readily available.

Two: segment your data. A single breach shouldn't give attackers access to an entire network or infrastructure and a mother lode of proprietary data.

Three: stay updated on the threat bulletins that DHS and FBI put out. We regularly warn about the intrusions taking place against U.S. businesses and we advise private sector entities on how to protect themselves against those threats.

And four: teach folks, including your friends and family, what spear phishing looks like. So many times, bad actors get access to our systems and our information just by pretending to be someone else and then asking people to open an attachment or click on a link. It's simple but it is the single most important factor in infections. The Chinese, in particular, are cleaning us out because we know we're supposed to do those simple things and yet we don't do them.

This is not to say that these steps will eliminate all the risk and uncertainty that comes with using cyber for communication and commerce, but it will have an immediate positive impact on our vulnerabilities.

The two remaining steps are challenging and interconnected. The first is to improve our cyber literacy as an intelligence community, as a government, and as a nation. And second, empower people to excel in the realm of cyber. Not so simple.

You recall that Fortran team; their express goal was to open up coding to a whole community of people for whom programming was prohibitively complex. They recognized that the only way to really advance computer sciences and so many other disciplines was to increase the number of people participating in the conversation.

They applied themselves to diversifying the field of programming by lowering the barriers to entry and then sharing their technology advances with others. Essentially, they engineered a huge leap forward in cyber literacy, not unlike what you are all doing here today.

You are bringing people into the field, opening up pathways, and it is programs like this that will change the world. Because if we take the Fortran team as an example, we know that you don't have to have twenty years in programming under your belt to make a difference. You need to know that you're wanted and welcomed, and you need a chance to succeed.

Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

Which leads me to that second complicated step: empowerment. As managers, teachers, mentors we need to empower the next generation to succeed. We have to trust them when they want to take a smart risk and then give them the 'top cover' so they can fail sometimes.

On innovating, John Backus, the Fortran team leader said this: "You need the willingness to fail. You have to generate so many ideas and then you have to work very hard only to discover that they don't work. And you keep doing that over and over until you find one that does."

The team's willingness to persevere in spite of setbacks and doubts is only one part of that story. The other part is that they all had bosses, and mentors, and friends telling them that it was okay to fail. It was okay to take risks because each and every failure was a lesson learned. How else do we succeed in pioneering a new frontier if not by learning from our mistakes?

So as a community, we need to raise cyber literacy by giving more people the tools to participate in the cyber conversation. That's education, as you are doing here, and you're making great strides. Simultaneously, we absolutely must empower those who are brave enough to innovate and are willing to push themselves. And a big part of empowerment is allowing people to try, and to fail. So, those two things – increasing participation in the cyber conversation and empowerment – will help us, as a nation, foster the next generation of innovators and visionaries.

But there is another key element that will help us keep pace with those diverse threats that I mentioned earlier, and that is to be as diverse as the threats that we face. Diversity was key to the Fortran team's ability to overcome their own challenges and it is uniquely critical to our work in the Intelligence Community. Backus, the Fortran team leader, sought out people with diverse expertise because he wanted to fill his lab with folks whose thought processes were as different from his own as possible.

And defying all convention, he brought on a newly minted college graduate, Lois, a brilliant female mathematician who barely knew what coding entailed. But what Backus saw was someone who could approach the seemingly insurmountable problems associated with high-level programming with fresh eyes. As a result, supercomputing tasks like weather and climate modeling, and computational chemistry, economics and physics are possible because of the advent of high-level programming language and the foundational work of that Fortran team.

Initiatives like AU's Cyber Institute, teaching kids to code at an early age, and the 'Girls Who Code' movement are all about inclusivity, bringing that most diverse minds into computer science. In truth, all types of diversity matter for innovation to work; whether it's thought,

Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

experience, up-bringing, culture, language. And diversity is equally as fundamental for the Intelligence Community's work.

At the individual level, in my own experience as an engineer and program manager, I knew that I could anticipate and prevent the problems that *I* could think of, but what I had to worry about were the problems I didn't think of. I needed people with different experiences to find those problems, to ask the question that I did not.

All of our endeavors in the Intelligence Community will benefit from the fact that people who think differently are valued. If you speak a different language – including programming languages – or have a unique cultural background, you can bring something to the intelligence game.

We need operations officers who blend into their environment. You cannot look like me and operate on many of the streets of this world. We need analysts whose understanding of diverse global communities is equally as diverse. And we need people who see a new way of doing business, who can figure out how to ship tons of equipment to the far corners of the world faster than anyone else on the planet could. We need cyber experts who can stay at the cutting edge of technology, which is changing at an unprecedented pace and accelerating. Those are diversity needs very specific to the Intelligence Community and to our business.

Our job is to understand and explain the world around us; to assess, analyze, and respond to the events that impact our nation's priorities. We can't do that effectively if we are all following the same thought patterns. If you take a look back at intelligence failures over the years and decades, you will find that a lack of diversity played into our mistakes. If someone with a different perspective had been involved in so many of those cases that person could have asked the 'what if' question that might have avoided the failure.

Irving Janis, the psychologist credited for exposing the dangers of groupthink, actually used the Cuban Missile Crisis in 1962 to expose the pitfalls of homogeneity. In short, Janis concluded that diversity of thought, valuing the outside perspective, was essential to avoiding all-out devastation.

That is exactly why Director Clapper and I talk about intelligence integration every chance we get; because integration and diversity are not just 'nice to have.' They are imperative. They make us strong.

In fact, it is the very core of the ODNI's mission, bringing the best and most appropriate minds to bear on our toughest challenges. What that means is preserving the unique capabilities of the

Remarks as delivered by The Honorable Stephanie O'Sullivan Principal Deputy Director of National Intelligence

17 different intelligence entities and helping the entire community to leverage those diverse capabilities – not turning the Intelligence Community into a big, bland bowl of oatmeal.

But diversity and integration don't stop there. We need all of you. Integration cannot and does not end at the boundaries of the Intelligence Community. Our partnerships extend across the federal, state, and local governments and they depend on American innovation. With your partnership we can continue to stay ahead of those 'most diverse threats.'

So here's my pitch before we turn this into a conversation: yes, if you are an expert on cyber security or you speak four languages there is a place for you in the Intelligence Community, but if you are an accountant or a lawyer, if you have a mind for logistics, or you are studying to become an engineer, there is a place for you too. There is an interesting puzzle, a problem, a seemingly insurmountable challenge out there that we need you to solve.

And while we can't pay you what you might make in some private sector jobs, and we have some tough security requirements, what I can promise you is the chance to work next to some of the brightest, and most dedicated people, people you will respect, people who are motivated by something bigger than themselves. And together, we can tackle some of the most interesting and challenging issues facing our nation today.

As one of my first bosses told me when I first joined the Intelligence Community: "I promise you, you'll never be bored. You will experience every other emotion. But you will never be bored." He was right. The mission is unparalleled, and you can be a part of it.